

CLAIMS

1. A method of managing security in an enterprise, comprising:
detecting at periodic intervals events that correspond to user interactions with
5 computers connected to a network of the enterprise;
storing such events in a data facility;
organizing the events by user, by computer and by event type; and
presenting a summary of the events in a report, wherein a viewer of the report
may select the organization of the report by user, by computer and by event type.
10
2. A method of claim 1, wherein the report is in a graphical format.
3. A method of claim 1, further comprising limiting access to the report based on
a predetermined level of authority of the party seeking access.
15
4. A method of claim 1, wherein the events are selected from the group
consisting of keyboard event, a mouse event, an intellipoint event, a trackball event, a
cursor event, a screen event, sensor event, a touchpad event, a tablet event, a
touchscreen event, a joystick event, a pen event, a voice recognition event, and
20 biometric event.
5. A method of claim 1, wherein the user is selected from the group consisting of
an employee, a consultant, a teacher, a student, a government official, a patient, a
volunteer, an attendant, a team member, a system administrator, a contractor, a
25 vendor, a clerk, a cashier, a teller, a comptroller, an accountant, an attorney, a
financial officer, a principal, an administrator, a human resources employee, a broker,
a gaming employee, a guard, a banker, a government official, a trustee, a guardian, a
steward, an authorized user and a non-authorized user.
- 30 6. A method of claim 1, wherein the report relates to compliance with a policy of
the enterprise.

7. A method of claim 1, wherein the report relates to security of the enterprise.
8. A method of claim 1, wherein the report relates to performance of an objective
5 of the enterprise.
9. A method of claim 1, wherein the report relates to content viewed by the user,
the content selected from the group consisting of chat room content, content relating
to securities, insider trading information, content relating to gaming, pornographic
10 content, illegal content, vulgar content, prurient content, gambling content,
entertainment content, video game content, trade secret content, proprietary content,
engineering content, drug-related content, health-related content, a medical record, a
patient record, a financial record, account information, educational information,
15 indication of harassment, indication of a crime, indication of policy or regulatory non-
compliance, identification of a competitive entity, identification of an adverse entity,
identification of a specific individual, transcript information, access to an
employment-oriented website, content designated prohibited by policy, and trading
information.
- 20 10. A method of managing compliance with policies of an enterprise, comprising:
detecting at periodic intervals events that correspond to user interactions with
computers connected to a network of the enterprise;
storing such events in a data facility;
organizing the events by user, by computer and by event type; and
25 presenting a summary of the events in a graphical-format report, wherein a
viewer of the report may select the organization of the report.
11. A method of claim 10, further comprising limiting access to the report based
on a predetermined level of authority of the party seeking access.
- 30 12. A method of claim 10, wherein the events are selected from the group

consisting of keyboard event, a mouse event, an intellipoint event, a trackball event, a cursor event, a screen event, sensor event, a touchpad event, a tablet event, a touchscreen event, a joystick event, a pen event, a voice recognition event, and biometric event.

5

13. A method of claim 10, wherein the user is selected from the group consisting of an employee, a consultant, a teacher, a student, a government official, a patient, a volunteer, an attendant, a team member, a system administrator, a contractor, a vendor, a clerk, a cashier, a teller, a comptroller, an accountant, an attorney, a
10 financial officer, a principal, an administrator, a human resources employee, a broker, a gaming employee, a guard, a banker, a government official, a trustee, a guardian, a steward, an authorized user and a non-authorized user.

14. A method of claim 10, wherein the report relates to compliance with a policy
15 of the enterprise.

15. A method of claim 10, further comprising sending an alert if a user is suspected of committing a security violation based on the user interactions with the computer.

20

16. A method of claim 10, further comprising increasing the rate of capture of user interactions if a user is suspected of committing a security violation.

17. A method of claim 10, wherein the report relates to content viewed by the
25 user, the content selected from the group consisting of chat room content, content relating to securities, insider trading information, content relating to gaming, pornographic content, illegal content, vulgar content, prurient content, gambling content, entertainment content, video game content, trade secret content, proprietary content, engineering content, drug-related content, health-related content, a medical
30 record, a patient record, a financial record, account information, educational information, indication of harassment, indication of a crime, indication of policy or

regulatory non-compliance, identification of a competitive entity, identification of an adverse entity, identification of a specific individual, transcript information, access to an employment-oriented website, content designated prohibited by policy, and trading information.

5

18. A method of managing productivity of individuals operating within a business enterprise, comprising:

detecting at periodic intervals events that correspond to user interactions with computers connected to a network of the enterprise;

10 storing such events in a data facility;

organizing the events by user, by computer and by event type; and

presenting a summary of the events in a graphical-format report, wherein a viewer of the report may select the organization of the report.

15 19. A method of claim 18, further comprising limiting access to the report based on a predetermined level of authority of the party seeking access.

20. A method of claim 18, wherein the events are selected from the group consisting of keyboard event, a mouse event, an intellipoint event, a trackball event, a
20 cursor event, a screen event, sensor event, a touchpad event, a tablet event, a touchscreen event, a joystick event, a pen event, a voice recognition event, and biometric event.

21. A method of claim 18, wherein the user is selected from the group consisting
25 of an employee, a consultant, a teacher, a student, a government official, a patient, a volunteer, an attendant, a team member, a system administrator, a contractor, a vendor, a clerk, a cashier, a teller, a comptroller, an accountant, an attorney, a financial officer, a principal, an administrator, a human resources employee, a broker, a gaming employee, a guard, a banker, a government official, a trustee, a guardian, a
30 steward, an authorized user and a non-authorized user.

22. A method of claim 18, wherein the event relates to an employee's usage of the Internet.

23. A method of claim 22, further comprising providing an alert if an employee's
5 usage of the Internet exceeds a predetermined amount during a predetermined period of time.

24. A method of claim 18, wherein the report relates to content viewed by the user, the content selected from the group consisting of chat room content, content
10 relating to securities, insider trading information, content relating to gaming, pornographic content, illegal content, vulgar content, prurient content, gambling content, entertainment content, video game content, trade secret content, proprietary content, engineering content, drug-related content, health-related content, a medical record, a patient record, a financial record, account information, educational
15 information, indication of harassment, indication of a crime, indication of policy or regulatory non-compliance, identification of a competitive entity, identification of an adverse entity, identification of a specific individual, transcript information, access to an employment-oriented website, content designated prohibited by policy, and trading information.

20

25. A system for managing security in an enterprise, comprising:
a) a component for detecting at periodic intervals events that correspond to user interactions with computers connected to a network of the enterprise;

b) a data facility for storing the events detected by the agent; and

25 c) a reporting facility for organizing and reporting the events by user, by computer and by event type.

26. A system of claim 25, wherein the reporting facility generates a report in a graphical format.

30

27. A system of claim 25, further comprising a security facility for limiting access

to the report based on a predetermined level of authority of the party seeking access.

28. A system of claim 27, wherein the security facility comprises an encryption facility.

5

29. A system of claim 27, wherein the security facility comprises a password.

30. A system of claim 25, wherein the events are selected from the group consisting of keyboard event, a mouse event, an intellipoint event, a trackball event, a cursor event, a screen event, sensor event, a touchpad event, a tablet event, a touchscreen event, a joystick event, a pen event, a voice recognition event, and biometric event.

31. A system of claim 25, wherein the user is selected from the group consisting of an employee, a consultant, a teacher, a student, a government official, a patient, a volunteer, an attendant, a team member, a system administrator, a contractor, a vendor, a clerk, a cashier, a teller, a comptroller, an accountant, an attorney, a financial officer, a principal, an administrator, a human resources employee, a broker, a gaming employee, a guard, a banker, a government official, a trustee, a guardian, a steward, an authorized user and a non-authorized user.

32. A system of claim 25, wherein the reporting facility reports compliance with a policy of the enterprise.

25 33. A system of claim 25, wherein the reporting facility reports security events.

34. A system of claim 25, wherein the reporting facility reports on performance of an objective of the enterprise.

30 35. A system of claim 25, wherein the report facility reports on interaction by the user with content selected from the group consisting of chat room content, content

relating to securities, insider trading information, content relating to gaming,
pornographic content, illegal content, vulgar content, prurient content, gambling
content, entertainment content, video game content, trade secret content, proprietary
content, engineering content, drug-related content, health-related content, a medical
5 record, a patient record, a financial record, account information, educational
information, indication of harassment, indication of a crime, indication of policy or
regulatory non-compliance, identification of a competitive entity, identification of an
adverse entity, identification of a specific individual, transcript information, access to
an employment-oriented website, content designated prohibited by policy, and trading
10 information.

36. A system for managing compliance with policies of an enterprise, comprising:
an agent for detecting at periodic intervals events that correspond to user
interactions with computers connected to a network of the enterprise;
15 a data facility for storing such events by user, by computer and by event type;
and
a reporting facility for presenting a summary of the events in a graphical-
format report, wherein a viewer of the report may select the organization of the report.

20 37. A system of claim 36, further comprising a security facility for limiting access
to the report based on a predetermined level of authority of the party seeking access.

38. A system of claim 37, wherein the security facility comprises an encryption
facility.

25 39. A system of claim 37, wherein the security facility comprises a password.

40. A system of claim 36, wherein the events are selected from the group
consisting of keyboard event, a mouse event, an intellipoint event, a trackball event, a
30 cursor event, a screen event, sensor event, a touchpad event, a tablet event, a
touchscreen event, a joystick event, a pen event, a voice recognition event, and

biometric event.

41. A system of claim 36, wherein the user is selected from the group consisting of an employee, a consultant, a teacher, a student, a government official, a patient, a
5 volunteer, an attendant, a team member, a system administrator, a contractor, a vendor, a clerk, a cashier, a teller, a comptroller, an accountant, an attorney, a financial officer, a principal, an administrator, a human resources employee, a broker, a gaming employee, a guard, a banker, a government official, a trustee, a guardian, a steward, an authorized user and a non-authorized user.
- 10
42. A system of claim 36, wherein the reporting facility reports events relating to compliance with a policy of the enterprise.
43. A system of claim 36, further comprising a communication facility for sending
15 an alert if a user is suspected of committing a security violation based on the user interactions with the computer.
44. A system of claim 36, further comprising a dynamic facility of the agent for increasing the rate of capture of user interactions if a user is suspected of committing
20 a security violation.
45. A system of claim 36, wherein the report reporting facility reports content viewed by the user, the content selected from the group consisting of chat room content, content relating to securities, insider trading information, content relating to
25 gaming, pornographic content, illegal content, vulgar content, prurient content, gambling content, entertainment content, video game content, trade secret content, proprietary content, engineering content, drug-related content, health-related content, a medical record, a patient record, a financial record, account information, educational information, indication of harassment, indication of a crime, indication of
30 policy or regulatory non-compliance, identification of a competitive entity, identification of an adverse entity, identification of a specific individual, transcript

information, access to an employment-oriented website, content designated prohibited by policy, and trading information.

5 46. A system for managing productivity of individuals operating within a business enterprise, comprising:

an agent for detecting at periodic intervals events that correspond to user interactions with computers connected to a network of the enterprise;

a data facility for storing such events by user, by computer and by event type;

and

10 a reporting facility for presenting a summary of the events in a graphical-format report, wherein a viewer of the report may select the organization of a report generated by the reporting facility.

15 47. A system of claim 46, further comprising limiting access to the report based on a predetermined level of authority of the party seeking access.

20 48. A system of claim 46, wherein the events are selected from the group consisting of keyboard event, a mouse event, an intellipoint event, a trackball event, a cursor event, a screen event, sensor event, a touchpad event, a tablet event, a touchscreen event, a joystick event, a pen event, a voice recognition event, and biometric event.

25 49. A system of claim 46, wherein the user is selected from the group consisting of an employee, a consultant, a teacher, a student, a government official, a patient, a volunteer, an attendant, a team member, a system administrator, a contractor, a vendor, a clerk, a cashier, a teller, a comptroller, an accountant, an attorney, a financial officer, a principal, an administrator, a human resources employee, a broker, a gaming employee, a guard, a banker, a government official, a trustee, a guardian, a steward, an authorized user and a non-authorized user.

30

50. A system of claim 46, wherein the event relates to an employee's usage of the

Internet.

51. A system of claim 50, further comprising an alarm facility for providing an alert if an employee's usage of the Internet exceeds a predetermined amount during a
5 predetermined period of time.

52. A system of claim 46, wherein the report relates to content viewed by the user, the content selected from the group consisting of chat room content, content relating to securities, insider trading information, content relating to gaming, pornographic
10 content, illegal content, vulgar content, prurient content, gambling content, entertainment content, video game content, trade secret content, proprietary content, engineering content, drug-related content, health-related content, a medical record, a patient record, a financial record, account information, educational information, indication of harassment, indication of a crime, indication of policy or regulatory non-
15 compliance, identification of a competitive entity, identification of an adverse entity, identification of a specific individual, transcript information, access to an employment-oriented website, content designated prohibited by policy, and trading information.

20 53. A method of managing security in an enterprise, comprising:
detecting at periodic intervals events that correspond to user interactions with computers connected to a network of the enterprise;
storing such events in a data facility;
organizing the events by user, by computer and by event type;
25 permitting access by an individual to the stored events; and
logging events that indicate the nature of the access by the individual to the stored events.